Peut-on rêver d'une écriture impénétrable ?

Anne Canteaut

Inria, Paris

Crédit photo : US Army

Collège de France, colloque de rentrée, 21 octobre 2022

La cryptographie ou l'art de chiffrer

Chiffrement : écriture conçue pour rester inintelligible,
sauf pour un groupe de personnes légitimes.

Dualité du monde :

- utilisateurs légitimes
- adversaires

Avantage dont disposent les utilisateurs légitimes :

clef secrète de déchiffrement.

La cryptographie ou l'art de chiffrer

Chiffrement : écriture conçue pour rester inintelligible,
sauf pour un groupe de personnes légitimes.

Dualité du monde :

- utilisateurs légitimes, qui **déchiffrent** à l'aide de leur clef de déchiffrement,
- adversaires, qui tentent de **décrypter** sans connaître la clef.

Avantage dont disposent les utilisateurs légitimes :

clef secrète de déchiffrement.

Existe-t-il des chiffrements impossibles à décrypter ?

Secret de Polichinelle ?

Quelle partie du procédé de chiffrement doit être secrète ?

≪ La cryptographie militaire ≫ (1883), Auguste Kerckhoffs

Secret de Polichinelle ?

Quelle partie du procédé de chiffrement doit être secrète ?

≪ La cryptographie militaire ≫ (1883), Auguste Kerckhoffs

≪ Il faut que [le système] n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi.

Et ici j'entends par secret, non la clef proprement dite, mais ce qui constitue la partie matérielle du système : tableaux, dictionnaires ou appareils mécaniques quelconques qui doivent en permettre l'application. [...] Rien qu'à ce point de vue il y aurait lieu de condamner l'emploi du dictionnaire chiffré, qui est en usage aujourd'hui dans l'armée. ≫

La chimère de Kerckhoffs

≪ On m'objectera peut-être qu'il n'est guère possible d'établir un système complètement indéchiffrable. Il faut s'entendre : je sais très bien que vouloir dans ces conditions trouver un système **mathématiquement** indéchiffrable est chose mathématiquement impossible ; mais j'affirme [...] qu'on peut parfaitement combiner des systèmes, sinon mathématiquement, du moins matériellement indéchiffrables. ≫

Et pourtant...

William F. Friedman (1924)

≪All popular ideas to the contrary notwithstanding, the condition termed "**absolute indecipherability**" is by no means purely chimerical, or impossible of production, for the existence of but one case in which it can be demonstrated that such a condition has been produced is sufficient to establish the validity of the hypothesis, as well as of the possibility of the existence of other absolutely indecipherable systems.

One such case is exemplified in that type of cryptographic system known as the "running" or "continuous key" method.≫

L'indéchiffrabilité absolue ou la sécurité parfaite [Shannon 49]

Intercepter le message chiffré ne fournit aucune information sur le message clair.

≪ Quel que soit le message chiffré, la probabilité *a posteriori* de chacun des messages clairs est égale à sa probabilité *a priori*, indépendamment de la valeur du message chiffré. ≫

De manière équivalente, pour toute paire de messages clairs (m_1, m_2),
pour tout message chiffré c,

$$\Pr_K[E_K(m_1) = c] = \Pr_K[E_K(m_2) = c]$$

Le masque jetable [Vernam 1918-1926, Mauborgne ?]

clair	s	y	s	t	e	m	e	i	n	c	a	s	s	a	b	l	e
	18	24	18	19	4	12	4	8	13	2	0	18	18	0	1	11	4
clef	g	v	w	q	t	y	s	k	r	g	s	e	d	l	w	p	m
	6	21	22	16	19	24	18	10	17	6	18	4	3	11	22	15	12
chiffré	24	19	14	9	23	10	22	18	4	8	18	22	21	11	23	0	16
	y	t	o	j	x	k	w	s	e	i	s	w	v	l	x	a	q

Le masque jetable [Vernam 1918-1926, Mauborgne ?]

Un système mathématiquement indéchiffrable

clair	s	y	s	t	e	m	e	i	n	c	a	s	s	a	b	l	e
clef	g	v	w	q	t	y	s	k	r	g	s	e	d	l	w	p	m
chiffré	y	t	o	j	x	k	w	s	e	i	s	w	v	l	x	a	q

clair	a	u	c	u	n	e	i	n	f	o	r	m	a	t	i	o	n
clef	y	z	m	p	k	g	j	k	r	d	e	f	j	l	e	s	c
chiffré	y	t	o	j	x	k	w	s	e	i	s	w	v	l	x	a	q

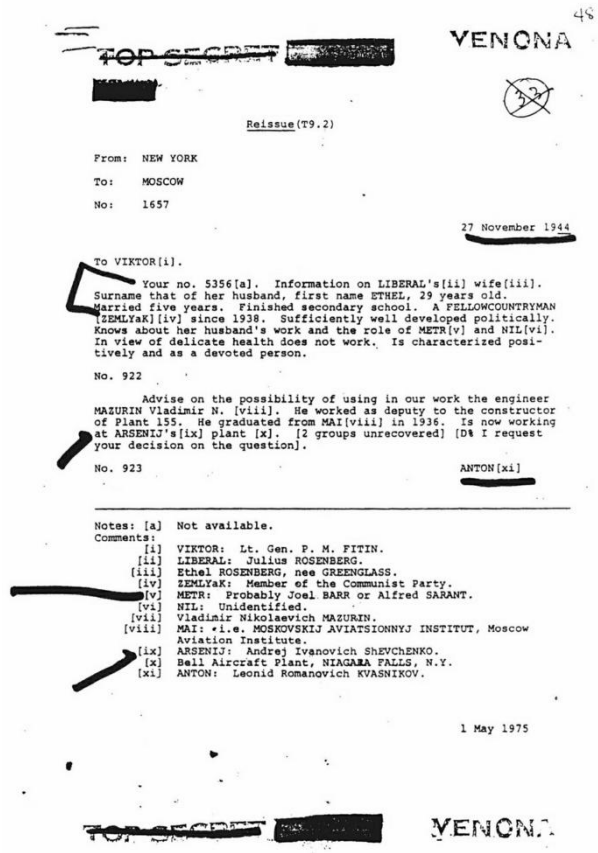
Chaque message chiffré peut correspondre à n'importe quel message clair ayant le même nombre de lettres.

→ Sécurité parfaite, à condition que la clef soit une suite aléatoire à usage unique.

Le projet Venona

≪ Pénurie ≫ de clefs dans les ambassades soviétiques aux USA pendant la Seconde Guerre mondiale

→ Analyse des communications des services diplomatiques et commerciaux soviétiques émises de 1940 à 1948.



TOP SECRET [redacted] VENONA

Reissue(T9.2)

From: NEW YORK

To: MOSCOW

No: 1657

27 November 1944

To VIKTOR[i].

Your no. 5356[a]. Information on LIBERAL's[ii] wife[iii]. Surname that of her husband, first name ETHEL, 29 years old. Married five years. Finished secondary school. A FELLOWCOUNTRYMAN [ZEMLYaK][iv] since 1938. Sufficiently well developed politically. Knows about her husband's work and the role of METR[v] and NIL[vi]. In view of delicate health does not work. Is characterized positively and as a devoted person.

No. 922

Advise on the possibility of using in our work the engineer MAZURIN Vladimir N. [viii]. He worked as deputy to the constructor of Plant 155. He graduated from MAI[viii] in 1936. Is now working at ARSENIJ's[ix] plant [x]. [2 groups unrecovered] [D% I request your decision on the question].

No. 923 ANTON[xi]

Notes: [a] Not available.
Comments:
[i] VIKTOR: Lt. Gen. P. M. FITIN.
[ii] LIBERAL: Julius ROSENBERG.
[iii] Ethel ROSENBERG, nee GREENGLASS.
[iv] ZEMLYaK: Member of the Communist Party.
[v] METR: Probably Joel BARR or Alfred SARANT.
[vi] NIL: Unidentified.
[vii] Vladimir Nikolaevich MAZURIN.
[viii] MAI: •i.e. MOSKOVSKIJ AVIATSIONNYJ INSTITUT, Moscow Aviation Institute.
[ix] ARSENIJ: Andrej Ivanovich ShEVChENKO.
[x] Bell Aircraft Plant, NIAGARA FALLS, N.Y.
[xi] ANTON: Leonid Romanovich KVASNIKOV.

1 May 1975

TOP SECRET [redacted] VENONA

La controverse sur l'inventeur du masque jetable

Vernam, Mauborgne and Friedman : The One-Time Pad and the Index of Coincidence, Steven M. Bellovin, 2016.

Deux systèmes proches mais de nature différente :

- le masque jetable avec une clef aléatoire, à usage unique, aussi longue que le message ;
- le schéma de Morehouse qui produit une clef pseudo-aléatoire de 999 000 caractères, en additionnant deux clefs aléatoires de longueur 999 et 1000, cassé par Friedman en 1919.

Le dilemme du cryptographe :

- assurer une sécurité parfaite ;
- se plier aux contraintes de mise en œuvre.

Une condition nécessaire à la sécurité parfaite [Shannon 49]

Théorème de Shannon.

Pour qu'un chiffrement assure une sécurité parfaite, il faut que le nombre de clefs possibles soit supérieur ou égal au nombre de messages clairs possibles.

Crédit photo : US Army

⟶ En théorie, tous les systèmes utilisés dans la pratique peuvent être décryptés.

De l'importance de la cryptanalyse

Mesure de l'effort requis pour ≪ casser ≫ le chiffrement.

≪ Casser ≫ :

- décrypter, i.e. retrouver le message clair à partir du message chiffré.
- retrouver la clef de déchiffrement à partir de la connaissance de certains couples clairs-chiffrés.

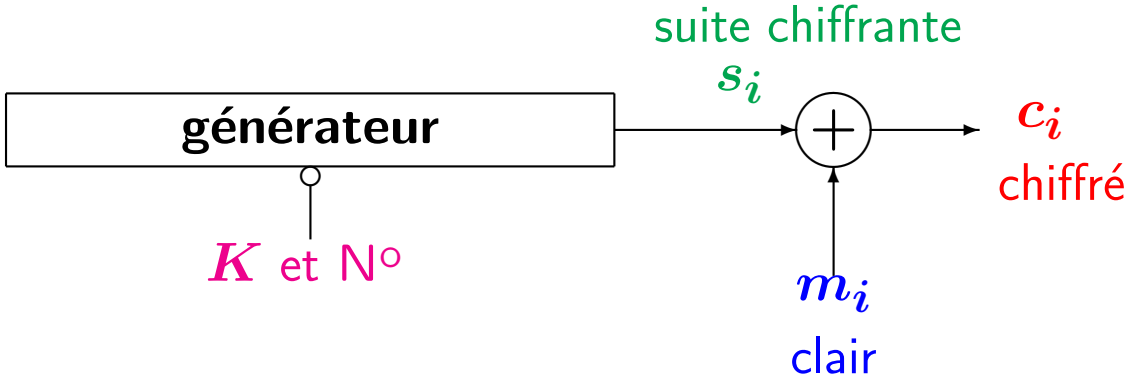
≪ Effort ≫ :

- temps de calcul
- quantité de mémoire
- quantité de données

$\longrightarrow$ Indispensable pour dimensionner le chiffrement, évaluer sa marge de sécurité.

Les versions affaiblies du masque jetable

La suite chiffrante est une suite pseudo-aléatoire produite par un automate déterministe à états finis à partir d'une clef secrète plus courte.



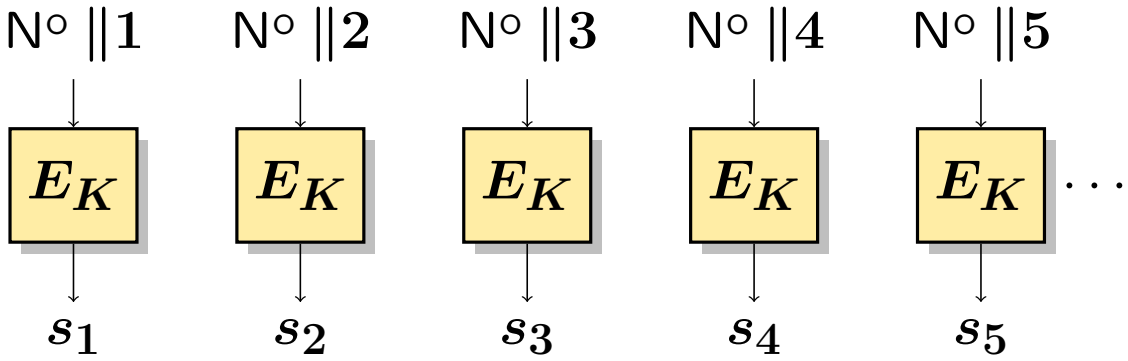
Critère de sécurité : on ne peut pas distinguer la suite générée d'une suite aléatoire en un coût inférieur à celui nécessaire pour essayer toutes les clefs.

Exemple : le mode COMPTEUR [Diffie-Hellman 1979, standard NIST 2001]

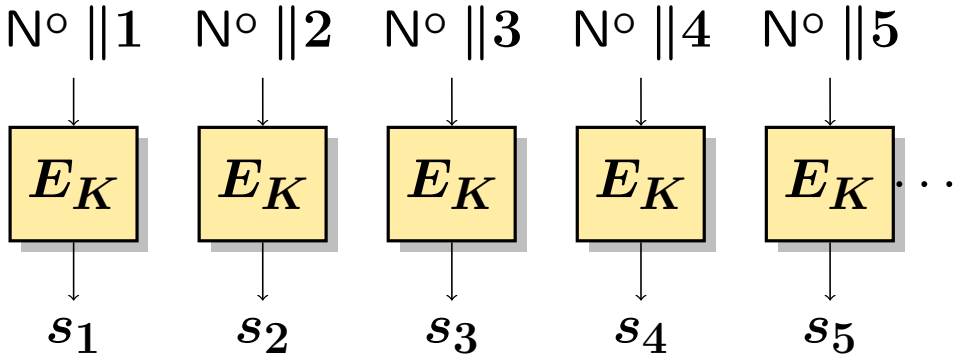
À partir d'un chiffrement par blocs sur les mots de n bits, où $n \in \{64, 128, 256\}$

Soit $\{E_K : K \in \mathcal{K}\}$ un ensemble de fonctions bijectives opérant sur des mots de n bits, et se comportant comme des bijections aléatoires (e.g. AES).

Génération d'une suite pseudo-aléatoire :



Analyse de la sécurité du mode COMPTEUR



- Les L blocs s_i générés sont distincts.
- S'ils étaient choisis au hasard, une telle situation se produit avec probabilité environ

$$1 - \frac{L^2}{2^{n+1}} \text{ (paradoxe des anniversaires).}$$

$\longrightarrow$ La longueur de la suite doit être très inférieure à $2^{n/2}$ blocs
(i.e. à 32 Go pour $n = 64$).

Peut-on exploiter cette propriété ?

Si $L \geq 2^{n/2}$, on peut retrouver un bloc de message clair grâce à un algorithme efficace pour résoudre le problème de la différence manquante [Leurent, Sibleyras 18].

En conclusion

Pour reformuler l'assertion de Kerckhoffs :

Trouver un système mathématiquement indéchiffrable est chose

- mathématiquement possible ;
- matériellement impossible.

Le caractère ≪ indéchiffrable ≫ d'un système de chiffrement ne peut être mesuré que par un effort public, soutenu et continu de cryptanalyse.